Teste avançado da proteção do malware ESA (ampère)

Índice

Introdução

Este documento descreve como testar e para verificar as características avançadas da proteção do malware (ampère) de Cisco envie por correio eletrónico a ferramenta de segurança (ESA).

Teste o ampère no ESA

Com a liberação de AsyncOS 8.5 para o ESA, o ampère executa varreduras da reputação do arquivo e análise do arquivo a fim detectar o malware nos acessórios.

Chaves de recurso

A fim executar o ampère, você deve ter uma chave de recurso válida e ativa para a **reputação do arquivo** e **arquivar a análise em** seu ESA. Visite **chaves de recurso do sistema Administration> no** GUI, ou use **featurekeys no** CLI, a fim verificar as chaves de recurso.

Serviços de segurança

A fim permitir o serviço do GUI, navegue aos **Serviços de segurança > à reputação e à análise do**

arquivo. Do CLI, você pode executar o **ampconfig**. Submeta e comprometa suas mudanças à configuração.

Políticas do correio recebido

Uma vez que você permitiu o serviço, você deve ter este serviço amarrado a uma política do correio recebido.

1. Navegue **para enviar políticas > políticas do correio recebido**.
2. Selecione sua **política padrão** ou política preconfigured como necessária. **A coluna de proteção avançada do malware no** correio recebido policia indicadores da página.
3. Selecione o link dos **enfermos** para a coluna, e **permita a reputação do arquivo** e **permita a análise do arquivo na** página das opções.
4. Você pode fazer todos os realces mais adicionais da configuração à exploração da mensagem, às ações para acessórios un-scannable, e às ações para mensagens positivamente identificadas, como necessários.
5. Submeta e comprometa suas mudanças à configuração.

Teste

Neste tempo, sua política do correio recebido é permitida de fazer a varredura e detectar do malware. Você deve ter uma amostra verdadeira do malware com que para testar. Se você precisa exemplos válidos, visite o instituto europeu para a página (eicar) das transferências da pesquisa do Antivirus do computador.

> Cuidado: Cisco não pode ser guardado responsável quando estes arquivos ou seu varredor AV em combinação com estes arquivos causam todo o dano a seu computador ou ambiente de rede. VOCÊ TRANSFERE ESTES ARQUIVOS A SEU PRÓPRIO RISCO. Transfira estes arquivos somente se você é suficientemente seguro no uso de seus varredor AV, ajustes do computador, e ambiente de rede. Esta informação é fornecida como uma cortesia para finalidades do teste e da reprodução.

Com o uso de um válido uma conta de email preconfigured, envia o acessório com de seus ESA e processamento normal. Você pode usar o CLI do ESA, e os **mail_logs da cauda** a fim monitorar o correio como ele processam. Você verá o ID de mensagem (MEADOS DE) alistado nos logs do correio. A saída similar a esta indica:

```
Thu Sep 18 16:17:38 2014 Info: New SMTP ICID 16488 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 16:17:38 2014 Info: ICID 16488 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 16:17:38 2014 Info: Start MID 1653 ICID 16488
```

```
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 From: <joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 ICID 16488 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 Message-ID '<BLU437-SMTP10E1315A60354F2
906677B9DB70@phx.gbl>'
Thu Sep 18 16:17:38 2014 Info: MID 1653 Subject 'Your Daily Update''
Thu Sep 18 16:17:38 2014 Info: MID 1653 ready 2313 bytes from
<joe_user@hotmail.com>
Thu Sep 18 16:17:38 2014 Info: MID 1653 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Sep 18 16:17:38 2014 Info: ICID 16488 close
Thu Sep 18 16:17:39 2014 Info: MID 1653 interim verdict using engine:
CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 using engine: CASE spam negative
Thu Sep 18 16:17:39 2014 Info: MID 1653 AMP file reputation verdict : MALWARE
Thu Sep 18 16:17:39 2014 Info: Message aborted MID 1653 Dropped by amp
Thu Sep 18 16:17:39 2014 Info: Message finished MID 1653 done
```

O exemplo anterior mostra que o ampère detectou o acessório do malware e **o deixou cair** como a ação final pelas configurações padrão.

Os mesmos detalhes são considerados igualmente no rastreamento de mensagem do GUI:

Se você escolhe entregar o malware positivamente identificado, ou outras opções avançadas na configuração ampère das políticas do correio recebido, você pôde ver este correio processar o resultado:

```
Thu Sep 18 21:54:30 2014 Info: MID 1655 AMP file reputation verdict : MALWARE
Thu Sep 18 21:54:30 2014 Info: MID 1655 rewritten to MID 1656 by AMP
```

A sentença da reputação é ainda positiva para o **MALWARE** como mostrado. A ação reescrita é pelas ações da alteração da mensagem e prepending da linha de assunto de **[ADVERTINDO: MALWARE DETECTADO]**.

Um arquivo limpo, ou um arquivo que não seja identificado no tempo de processamento como o malware, têm esta sentença escrita aos logs do correio:

```
Thu Sep 18 21:58:33 2014 Info: MID 1657 AMP file reputation verdict : CLEAN
```

Rastreamento de mensagem avançado para mensagens AMP+

Igualmente do GUI, quando você usa o rastreamento de mensagem e o menu suspenso avançado, você pode escolher procurar diretamente por uma mensagem positiva da proteção avançada do malware:

Relatórios avançados da proteção do malware

Do ESA GUI, você igualmente vê o relatório seguir para mensagens positivamente identificadas com o ampère. Navegue **para monitorar > avançou a proteção do malware** e alteram o intervalo de tempo como necessário. Você vê agora similar, com os exemplos anteriores para a entrada:

Troubleshooting

Se você não vê sabido, o arquivo verdadeiro do malware que é feito a varredura positivamente pelo ampère, reviu o correio entra a ordem para assegurar que um outro serviço não tomou a ação na mensagem e/ou no acessório antes que o ampère fez a varredura da mensagem.

Do exemplo mais adiantado usado, quando Sophos anti-vírus é permitido, realmente trava e toma a ação no acessório:

```
Thu Sep 18 22:15:34 2014 Info: New SMTP ICID 16493 interface Management
(192.168.0.199) address 65.55.116.95 reverse dns host blu004-omc3s20.hotmail.com
verified yes
Thu Sep 18 22:15:34 2014 Info: ICID 16493 ACCEPT SG UNKNOWNLIST match sbrs
[-1.0:10.0] SBRS 5.5
Thu Sep 18 22:15:34 2014 Info: Start MID 1659 ICID 16493
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 From: <joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 ICID 16493 RID 0 To:
<any.one@mylocal_domain.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 Message-ID '<BLU437-SMTP2399199FA50FB
5E71863489DB40@phx.gbl>'
Thu Sep 18 22:15:34 2014 Info: MID 1659 Subject 'Daily Update Final'
Thu Sep 18 22:15:34 2014 Info: MID 1659 ready 2355 bytes from
<joe_user@hotmail.com>
Thu Sep 18 22:15:34 2014 Info: MID 1659 matched all recipients for per-recipient
policy DEFAULT in the inbound table
Thu Sep 18 22:15:35 2014 Info: ICID 16493 close
Thu Sep 18 22:15:35 2014 Info: MID 1659 interim verdict using engine:
CASE spam negative
Thu Sep 18 22:15:35 2014 Info: MID 1659 using engine: CASE spam negative
Thu Sep 18 22:15:37 2014 Info: MID 1659 interim AV verdict using Sophos VIRAL
Thu Sep 18 22:15:37 2014 Info: MID 1659 antivirus positive 'EICAR-AV-Test'
Thu Sep 18 22:15:37 2014 Info: Message aborted MID 1659 Dropped by antivirus
Thu Sep 18 22:15:37 2014 Info: Message finished MID 1659 done
```

Os ajustes de configuração anti-vírus de Sophos na política do correio recebido são ajustados **para deixar cair** para mensagens contaminadas vírus. Nesta instância, o ampère é alcançado nunca para fazer a varredura ou tomar da ação no acessório.

Entretanto, esse nem sempre é o caso. Uma revisão dos logs do correio e dos ID de mensagem (MIDs) pôde ser precisada a fim assegurar que um outro serviço OU um filtro do índice/mensagem não tomou a ação contra o MEADOS DE antes do ampère que processa e uma ação foi alcançada.

Informações Relacionadas

- Cisco envia por correio eletrónico a ferramenta de segurança - Guias do utilizador final
- Suporte Técnico e Documentação - Cisco Systems